1 <u>**CLAIMS**</u>

2

3 We claim:

1   1.   A method comprising:

2   generating a first key component;

3   generating an encryption key using the first key component, a token

4 key and a personal identification number (PIN);

5   encrypting data using the encryption key;

6   sending the data encrypted with the encryption key to a server along

7 with the first key component.

1   2.   The method defined in Claim 1 further comprising receiving

2 the token key from a service provider.

1   3.   The method defined in Claim 1 further comprising the server

2 storing the first key component and the data encrypted with the encryption

3 key.

1   4.   The method defined in Claim 1 wherein the token key is

2   unique for each user.

1   5.   The method defined in Claim 1 wherein the first key

2   component is unique for each data entry stored by the server.

1   6.   A method comprising:

2   encrypting data using the encryption key generating using a first key

3   component, a token key and a personal identification number (PIN);

4   storing data encrypted using the encryption key; and

5   regenerating the encryption key after accessing the encrypted data to

6   decrypt the encrypted data therewith.

1   7.   The method defined in Claim 6 further comprising disabling

2   the token.

1   8.   The method defined in Claim 7 wherein the token is disabled if

2   lost.

1   9.   The method defined in Claim 7 wherein the token is disabled if

2   compromised.

1   10.   The method defined in Claim 7 further comprising re-enabling

2   the token.

1   11.   The method defined in Claim 6 wherein the token ID

2   comprises an alpha-numeric string.

1   12.   The method defined in Claim 11 wherein the token key

2   comprises a randomly generated number.

1   13.   The method defined in Claim 11 wherein either or both of the

2   token key and PIN comprises biometric data.

1   14.   The method defined in Claim 11 wherein the token key is the

2   same for all tokens used by the user.

1   15.   The method defined in Claim 6 further comprising:

2   monitoring browsing activities;

3   identifying web pages containing a form; and

4   inserting content into the form.

1   16.   The method defined in Claim 15 wherein inserting content into

2 the form is performed automatically.

1   17.   The method defined in Claim 15 wherein inserting content into

2 the form is performed with user confirmation.

1   18.   The method defined in Claim 15 further comprising allowing a

2 user to select the form to fill in.

1   19.   The method defined in Claim 15 further comprising allowing a

2 user to select a variant of the form to fill in.

1   20.   A method comprising:

2   retrieving a key component and encrypted data from a server;

3   recreating an encryption key using the key component, a token key

4   and a personal identification number (PIN); and

5   performing a decryption operation on the encrypted data using a

6   decryption key based on the encryption key used to encrypt the encrypted

7   data.

1   21.   A method for authentication comprising:

2   generating authentication data for a user based on a token key and a

3   personal identification number (PIN), the token key being unique to the

4   user; and

5   receiving a confirmation indicating that the authentication data has

6   been verified.

1   22.   A method comprising:

2   accessing encrypted data from a server;

3   decrypting the encrypted data using a token and a user-specific PIN

4   to be accessed.

1   23.   The method defined in Claim 22 wherein the token comprises

2   a token identifier (ID) and a token key.

1   24.   The method defined in Claim 22 wherein the token comprises

2   a utility to manage data depending on data type.

1   25.   The method defined in Claim 24 wherein the utility operates

2   on data in response to explicit user command or by automatically

3   monitoring applications producing and/or consuming data of that type.

1   26.   The method defined in Claim 25 wherein the utility handles

2   password data.